UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/312,150	05/14/1999	PHILIP J. MIRE	M-7219-US	2203

7590 12/20/2006

DAVID L. McCOMBS
HAYNES and BOONE, LLP
901 MAIN STREET
SUITE 3100
DALLAS,, TX 75202-3789

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/20/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/312,150	MIRE, PHILIP J.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,7-12,18-22 and 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,7-12,18-22 and 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 6 October 2006.

2. Claims 1, 7-12, 18-22 and 30 are pending in the application.

3. Claims 1, 7-12, 18-22 and 30 have been rejected.

4. Claims 2-6, 13-17 and 23-29 have been cancelled.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6 October 2006 has been entered.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 7-12, 18-22 and 30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1, 7-12, 18-22 and 30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Independent claims 1, 12 and 30 recite the limitations of "encrypting the session key, with a public key of the fist user using an asymmetric encryption routine, for storage as a first user key blob," "encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob," "decrypting the user key blob using the asymmetric encryption routine proving the first system with access to the session key". All three limitations recite a "key blob". However, the examiner finds no support in the original specification for a "key blob".

Independent claims 1, 12 and 30 recite "a session key randomly generated". However, after a careful review of the specification, the examiner finds no support in the original specification for a session key that was randomly generated.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 7, 8, 12, 18, 19 and 30 are rejected under 35 U.S.C. 102(e) as being anticipated by Albanese et al U.S. Patent No. 6,002,768.

As to claim 1, Albanese et al discloses a method for encrypting data, the method comprising:

providing a first data processing system for a first user and a second data processing system for a second user [column 7, lines 7-28];

providing a session key randomly generated by the second system for use in encrypting original data [column 5, lines 14-30];

encrypting the data using the session key and a symmetric encryption routine [column 9, lines 37-43];

encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob [column 9, lines 37-43];

encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob [column 9, lines 37-43];

storing a first user private key on any media [column 4, lines 20-36];

decrypting the user key blob using the asymmetric encryption routine providing the first system with access to the session key [column 6, lines 31-44]; and

the first system decrypting the data using the symmetric encryption routine and securely transmitting the data to the first system [column 6, lines 31-44].

As to claims 7 and 18, Albanese et al discloses storing the first user's private key on a data storage medium coupled to the destination data processing system [column 8, lines 4-14].

As to claims 8 and 19, Albanese et al discloses storing the master private key on a data storage medium coupled to the destination data processing system [column 7, lines 7-28].

As to claim 12, Albanese et al discloses a method for encrypting data, the method comprising:

providing a first data processing system for a first user and a second data processing system for a second user [column 7, lines 7-28];

providing a session key randomly generated by the second system for use in encrypting original data [column 5, lines 14-30];

encrypting the data using the session key and a symmetric encryption routine [column 9, lines 37-43];

encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob [column 9, lines 37-43];

encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob [column 9, lines 37-43];

storing a first user private key on any media [column 4, lines 20-36];

decrypting the user key blob using the asymmetric encryption routine providing the first system with access to the session key [column 6, lines 31-44];

the first system decrypting the data using the symmetric encryption routine and securely transmitting the data to the first system [column 6, lines 31-44]; and

a third party gaining access to the data using a master private key to decrypt the master key blob using the asymmetric encryption routine and gain access to the original data [column 9, lines 37-43].

As to claim 30, Albanese et al discloses a method for encrypting data, the method comprising:

providing a first data processing system for a first user and a second data processing system for a second user [column 7, lines 7-28];

providing a session key randomly generated by the second system for use in encrypting original data [column 5, lines 14-30];

encrypting the data using the session key and a symmetric encryption routine [column 9, lines 37-43];

encrypting the session key, with a public key of the first user using an asymmetric encryption routine, for storage as a first user key blob [column 9, lines 37-43];

encrypting the session key, with a master public key using the asymmetric encryption routine, for storage as a master key blob [column 9, lines 37-43];

storing a first user private key on any media [column 4, lines 20-36];

decrypting the user key blob using the asymmetric encryption routine providing the first system with access to the session key [column 6, lines 31-44];

the first system decrypting the data using the symmetric encryption routine and securely transmitting the data to the first system [column 6, lines 31-44]; and

a third party gaining access to the data using a master private key to decrypt the master key blob using the asymmetric encryption routine and gain access to the original data [column 9, lines 37-43].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 9, 10, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albanese et al U.S. Patent No. 6,002,768 as applied to claims 1 and 12 above, and further in view of Dillaway et al U.S. Patent No. 5,742,756.

As to claims 9 and 20, Albanese et al does not teach retrieving the first user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [figure 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al so that the first user's private key is

stored on a smart card coupled to the destination node. The private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al by the teaching of Dillaway because it utilizes a smart card to perform critical cryptography operations. The smart Card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart Card, and required cryptographic operations are performed on the smart Card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

As to claims 10 and 21, Albanese et al does not teach retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.

Dillaway teaches private key stored on a smart card utilizing a smart card reader coupled to the destination data processing system [figure 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al so that the master private key is stored on a smart card coupled to the destination node. The master private key is only retrieved when the smart card is inserted into the smart card reader.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al by the teaching of Dillaway because it utilizes a smart card to perform critical cryptography operations. The smart card can be programmed or otherwise configured to never expose the user's private keys. Rather than providing a private key to the user's computer, the key is held within the smart card, and required

cryptographic operations are performed on the smart card itself. This makes it impossible for hostile code to obtain the private key [column 3, lines 24-31].

10. Claims 11 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albanese et al U.S. Patent No. 6,002,768 as applied to claims 1 and 12 above, and further in view of Kruys U.S. Patent No. 5,555,309.

As to claims 11, 22 and 29, Albanese et al does not teach utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

Kruys teaches a plurality of master keys [column 2, lines 56-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al so that there would have been a plurality of public and private master keys to decrypt the encrypted session keys. There would have been multiple session keys so there would have been a public/private master key set to encrypt and decrypt the session keys.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Albanese et al by the teaching of Kruys because it utilizes master keys, each one of which is unique to a respective domain member, and is arranged to protect the respective member vector key of each domain member [column 3, lines 55-62].

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
December 13, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100